

The

Supporter's Security

Security Magazine Issued By Electronic Horizons Foundation (Issue 1)

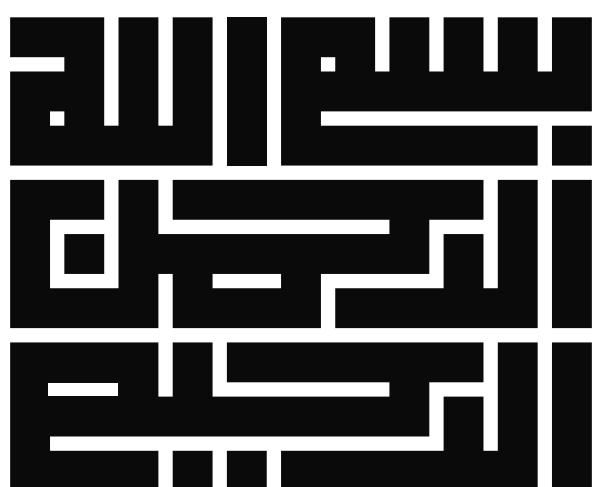
Introduction
**to smartphone
security**

Basics of protection
in iOS

Basics of protection
in Android OS

Introduction
**to computer
security**





CONTENT

Introduction	04
Introduction to smartphone security	06
Basics of protection in Android OS	10
Basics of protection in iOS	14
Your security on the internet	16
Wrong security practices	18
Introduction to computer security	20
Guide to Whonix OS	22



Introduction

It is not hidden from anyone How far technological development has reached in all fields of life of war and peace, led by polytheists, and they have the upper hand of it, they work their efforts day and night to use it against the religion of Allah, and humiliate the Muslims, so that they become under their control and mercy, and move under their surveillance, so their dictatorship increased on the servants of Allah and intensified. Muslims in general surrender to their bitter reality except those, the people of determination who used their times to learn how they repel their enemies, and spread the religion of Allah, and protect their brothers.

And Islam has obligated in such a case that Muslims should learn and prepare what strengthens them. The Almighty said: "And prepare for them whatever



you can of power.” One of the most important tools of our time is Information technology , which is the language of the age that runs most of the work fields, and its fields are multiple. Some of it needs specialization and long study, and some of it needs some serious attention, and Muslims are in such big need for both of them, the need is urgent, and you need a determination like Zaid bin Haritha, may Allah be pleased with him, he said: “The Messenger of Allah, Peace be upon him and his family, So I learned a book of Jews, and he said: I swear of Allah name that I do not trust the Jews on my book, so I learned it, and only half month passed and I learned it very well, I was writing for him, and read for him»

This is the order of the Prophet, may Allah prayers and peace be upon him, to Zaid bin Haritha, may Allah be pleased with him, by learning the language of his enemy, as soon as the need arises, and he worked hard and sincerely until he mastered it, so Allah preserved the words of the Prophet, may Allah prayers and peace be upon him, by him from distortion. Muslims must follow his legacy and learn and educate themselves to be safe from their enemy and fight it with its weapon. Today, the monotheists need to learn their digital security matters to be as far as possible from the eyes of intelligence, to spread the correct creed and defend the people of truth, and this is what we care about in the Electronic Horizons Foundation and we hope to be a help to the monotheists in this field, We are inside a fierce war, our sites and accounts in social media got deleted because the intelligence services realize the danger of Muslims gaining security awareness, which will make it difficult to track them and cut off the ways for them to arrest the monotheists, but we do not leave this field, Allah willing, until Allah decides what needs to be done, and we ask Allah to bless what we offer and make it pure for his face, praise To Allah, Lord of the worlds



Introduction to smartphone security

Smartphones have revolutionized the information technology world, where dozens of international companies are competing to manufacture billions of smartphones around the world, and phones have become accessible to all, and users have relied on them to manage their personal and administrative business. These changes have not only occurred in Western society but have also occurred in the Muslim and supporter community of monotheism, where many of the brothers and the Mujahideen started to use smartphones to communicate, publish, plan and work without knowing the real security risks they face.

When we talk about smartphones, there are dozens of manufacturers, but they depend on the Android operating system and iOS for iPhone and iPad devices, these technical companies that have a market value of billions of dollars do not depend on the manufacture of phones only, but they are interested in obtaining your data from your use of the phone, for smartphones know Everything you do during your day, it charts a pattern for your life, communication, and work style, and knows when to sleep, when to wake up, where to go, what to send, and with whom to communicate, and the manufacturers benefit from this data, which smartphones secretly send to technical corporate servers as it uses it to target you with advertising and advertisements and sell it to third parties, as well as governments and intelligence agencies that use this information in investigations, and technical companies cooperate with the security services under international law.

Local telecom companies also benefit from your use of smartphones, as telecommunications companies obtain valuable information and data from your activity on the Internet such as phone calls that you make and receive, text messages and geographical location coordinates within the coverage of cell towers and the websites that you visit and browse (without the use of VPN or Tor services))

The Mujahideen have been warned more than once about the danger of smartphones, which led to the arrest of many brothers due to the security negligence, so you must realize as a supporter of the truth that the security measures that need to be applied for you are completely different from the security measures used by anyone else, Understand the security threats facing you and how to choose the appropriate tools and methods to conduct your business and bypass electronic control, which includes every device connected to the Internet or cellular networks now.

Therefore, we advise the brothers to use computers instead of smartphones in the media work. As for those who cannot afford the cost of purchasing a computer or the use of the computer is not available in their current situation, here are security guidelines to reduce the security risks to which you are exposed - Allah willing -:

Note: If you are monitored by intelligence agencies, do not use the phone at all except to deceive the intelligence agencies by creating fake accounts on communication networks and applications that contradict your thoughts and beliefs - with the recommendation to stay away from suspicious contacts - and use the computer in media work and the support the Mujahideen

And if you are not under the watch of the intelligence agencies, do not let suspicious a chance to scare you because of your security and makes you stop from what is your duty toward your religion and your nation, then trust Allah and do what is available for you according to the security measures outlined

Use a new phone and beware of using a personal phone for media work.

Many brothers use personal phones for media work and publishing, which exposes them to dangerous security threats such as access to applications installed on the phone's identification data and associated with other personal accounts, and if your phone is compromised, the attacker will get all your personal information, which will be a treasure of information, and clicking on Malicious links will reveal your identity through the internet service provider, who knows the data which registered of the SIM cards that you entered in your phone, the number of SIM cards and the coordinates of your geographical location through cell towers, and therefore you must allocate a device for media work only and never use it for any personal use.

Sim cards

The SIM cards give the service provider in your country the authority to track you 24 hours within the coverage area of the cell towers. The service provider can also know the data of the SIM card that you use and the number of SIM cards that you inserted into the phone, so avoid using SIM cards at all in your phone.

Buying smartphones

Do not use your personal data when purchasing a smartphone for media work

Choosing the right phone

Smartphone manufacturers (Android) support phones with security updates for only three years from the date of manufacturing the phone, in order to compel users to always buy newer versions, however some companies do not provide monthly security updates, but some companies delay the issuance of the security patches that fix security vulnerabilities for more than three months and six months, which exposes you to the risks of penetration, therefore choosing the phone that you want to use in the media work should be very carefully and not according to the common devices.

Because the Android system is open source, there are many operating systems based on Android, which are known as «Custom Rom», including:

1- GrapheneOS operating system (recommended)

A free and open source operating system built on Android and formerly known as Copperhead OS. The system developers aim to maintain the privacy and security of the user and supports a specific category of smartphones that contain security features in Hardware

2- LineageOS Operating System

An open source operating system based on Android that supports many smartphones and tablets, and does not contain Google services, the project developers aim to maintain the privacy of the user and provide security updates for the phones which do not get any more support from the manufacturers, a project that complements the Cyanogenmod project

3- Replicant operating system

A free and open source operating system, based on Android that respects the privacy of users and aims to replace all proprietary components into free open source components

4- PostmarketOS system

An open source operating system, free of charge for smartphones, and based on the Alpine Linux distribution, which is completely different from the operating systems based on Android, as if it is a mini Linux system for smartphones, as the system developers aim to support the smartphones which do not receive any more support from the manufacturers and provide security updates.

Before buying a phone, you must first choose the operating system that you want to use and suit your work, because each operating system has different features from the other and depends on support for a specific range of phones, for example the GrapheneOS operating system only supports Pixel phones currently because the Pixel phone hardware is compatible with running the system's security features

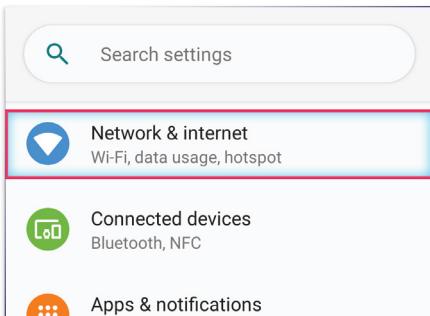
Note: Choosing the right phone for media work may be a confusing issue for some, so contact us via technical support accounts to guide you to the phone that is suitable for you.



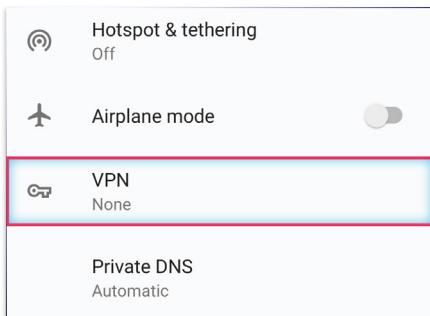
Horizons Designs

Basics of protection in Android OS

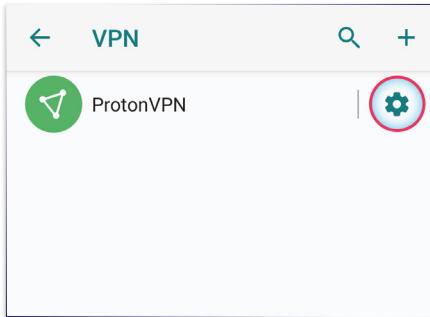
1



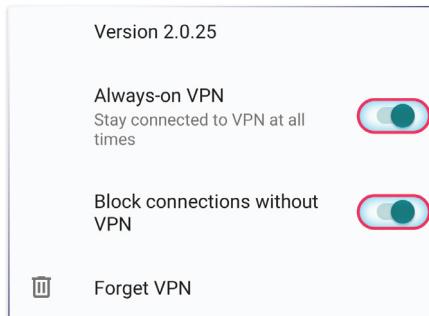
2



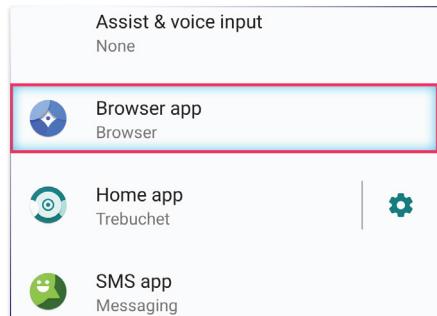
3



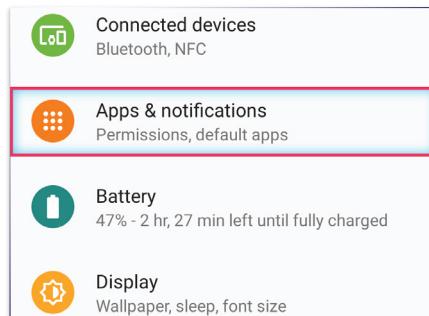
4



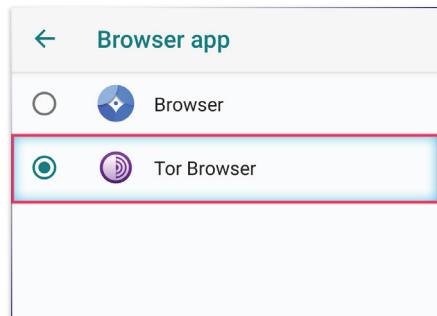
7



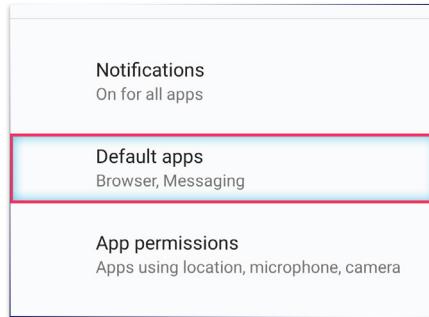
5



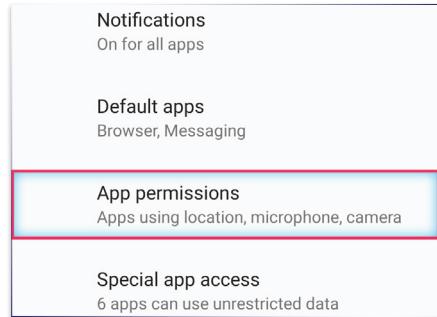
8



6



9



First: Activate Always-ON Feature

Android can start a VPN service when the device boots and keep it running while the device is on. This feature is called always-on VPN and is available in Android 7.0 (API Level 24) or higher, it's an important feature to prevent IP leaks

- 1 - Go to your phone settings and press on " Network & Internet "
- 2 - Navigate to the VPN section
- 3 - Click on " gear icon " as described
- 4 - Activate " Always-On VPN "
- Activate " Block Connections without VPN

Second: Choose the default browser to open links

There's many Suspicious Links and Websites on Social platforms you may click on any of them by mistake and if your security measures are weak your IP address could be revealed to a third party so it's recommended to use Tor Browser as your default browser

- 5 - Go to the Main Settings and Click on "Apps & Notifications"
- 6 - Choose "Default Apps"
- 7 - Click on "Browser App"
- 8 - Choose "Tor Browser"

Note : Install Tor Browser first from the official website or

F-droid before applying these settings

Third: Control App Permissions

Our phones contain dozens of apps, most of which require access privileges that violate your privacy! Older versions of Android do not provide permission control features, and Android 6.0 and higher has the future of managing apps permissions to control installed applications.

Make sure to prevent apps from accessing your phone's permissions related to your privacy as described in the explanation, and check that the

Basics of protection in Android OS

android

10

	Body Sensors 1 of 1 apps allowed
	Calendar 3 of 4 apps allowed
	Call logs 3 of 3 apps allowed
	Camera 4 of 4 apps allowed

11

	Calendar permission...		
	Calendar		
	Contacts		
	Email		
	Google Play services		

12

	Calendar	
	Calendar	
	Contacts	
	Email	
	Google Play services	

permissions of all Google-related apps and services are blocked.

9 - Go back to "Apps&Notifications" settings and click on "App Permissions"

10 - You can control the permissions of the applications installed on your phone, Apps should be prevented from accessing the permissions that violate your privacy such as (SMS - Body Sensors - Camera - Location - Microphone - Phone - Contacts - Call logs)

11 - If your phone contains Google services, be sure to prevent Google services from accessing Permissions that

13

	6 of 9 apps allowed
	SMS 4 of 5 apps allowed
	Storage 7 of 13 apps allowed
	Additional permissions 4 more

14

	Car information 0 of 0 apps allowed
	Read email attachments 0 of 1 apps allowed
	read instant messages 0 of 0 apps allowed
	write instant messages 0 of 0 apps allowed

15

	Notifications On for all apps
	Default apps Browser, Messaging
	App permissions Apps using location, microphone, camera
	Special app access 6 apps can use unrestricted data

violates your privacy.

Disable access for Google services, then click on the icon shown in the image to show hidden applications

12 - Choose "Show System" and block Google services

Note: You should review all Apps Permissions which installed on your phone

13 - After completing the settings, click on "Additional Permissions"

14 - Check those hidden applications are prevented from obtaining permission.

15 - Go back to "Apps & Notifications" Menu and press on

16

Battery optimization
Device admin apps
Display over other apps

17

	Find My Device Allow Find My Device to lock or erase a lost device
	Google Pay As a device administrator, Google Pay can help make your phone more secure

18

Premium SMS access
Unrestricted data
Install unknown apps

19

	Unrestricted data		
	Files		
	Gallery		
	Google Play services		

"Special App Access"

16 - Press on "Device admin apps"

17 - Disable "Find my device"

18 - Go back to special app access settings and "choose unrestricted data"

19 - Disable Google Play Services and press on options icon

20 - Press on "Show System" to show hidden system apps

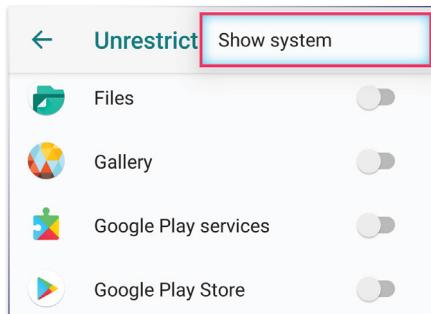
Make sure that all google apps is disabled

21 - Go back to special app access settings, Check every permission and disable google apps

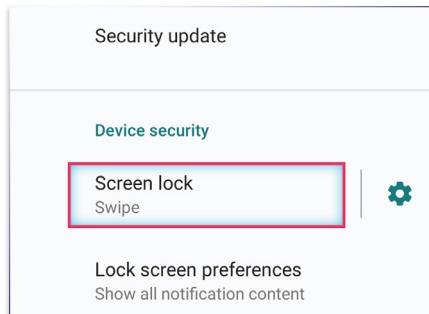
Basics of protection in Android OS

android

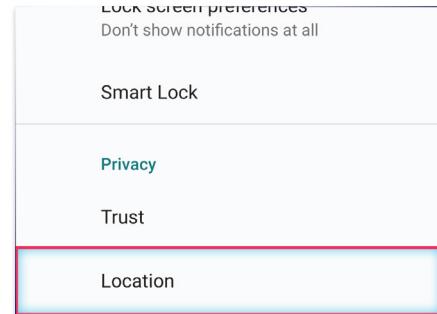
20



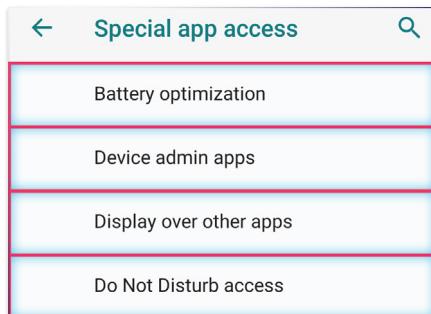
23



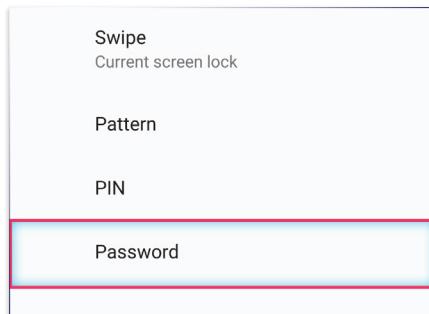
26



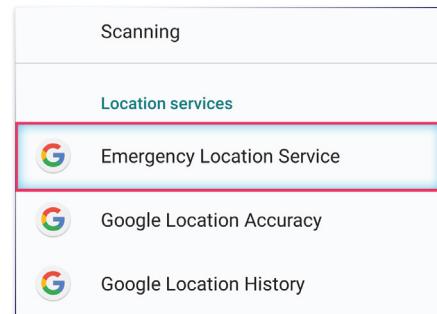
21



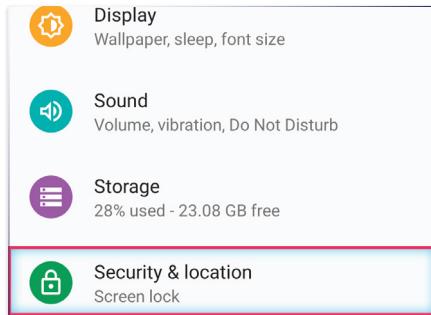
24



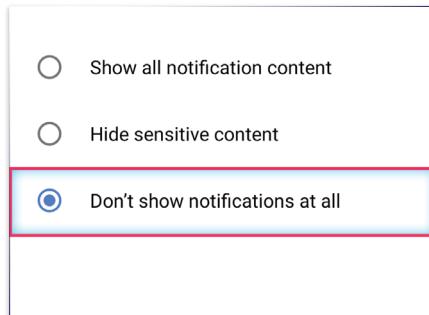
27



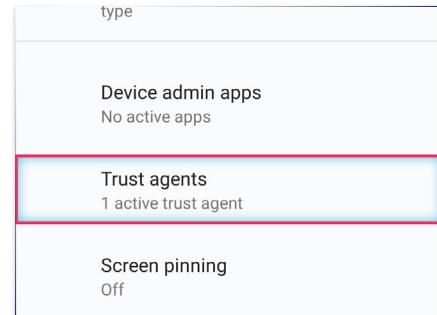
22



25



28



Fourth: Set a password for screen lock

Choose a strong password consisting of upper and lower case letters, numbers and symbols that are difficult to guess, and beware of using a fingerprint, face, pattern or PIN

22 - Press on "Security & location"

23 - Press on "Screen lock"

24 - Choose "Password"

25 - Choose "Don't show notifications at all"

Fifth: Preventing GPS tracking

Apps can accurately track the

coordinates of your geographical location when activating the geolocation services on the phone as well as with Google services, so make sure to disable them

26 - Click on "Location"

Press on "location"

27 - Disable "Use Location"

Disable "Emergency location Service"

28 - Go back to Security & location Settings and press on "Trust Agents"

29 - Disable "Smart lock"

Sixth: Prevent accounts sync

31 - Disable "automatically sync data"

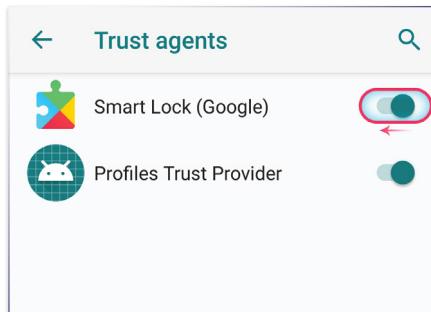
Seventh: Preventing applications from connecting to the Internet

You can not permanently get rid of Google services on your phone as it is one of the basic applications in Android phones, and it comes installed automatically from manufacturers, but you can get rid of Google services by installing another operating system that maintains your privacy like LineageOS, but these steps require some technical skills which we will explain in the next issue - In Sha Allah - but you

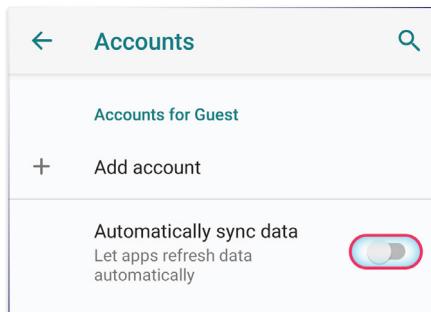
Basics of protection in Android OS

android

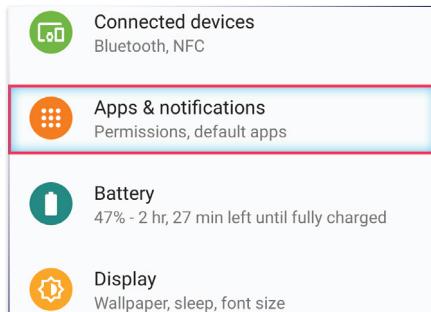
29



30



31



can currently block Google applications from connecting to the Internet, and this can reduce the security risks resulting from installing Google services on your phone.

32 - go to the main settings, then choose "Apps & notifications"

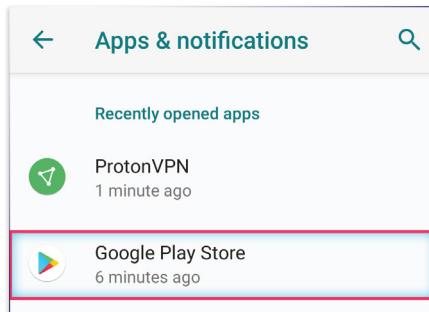
33 - choose the app that you want to ban from using the internet such as " Google play store"

34 - Press on " Data Usage"

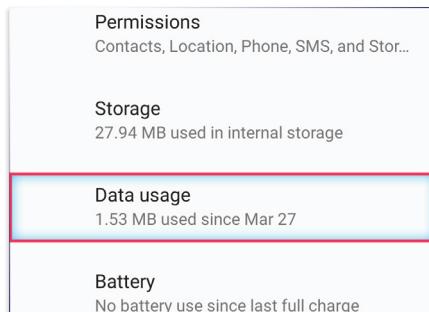
35 - You can block apps from connecting to the internet as shown in the screenshot by preventing them from using phone data or Wi-Fi

Note: Due to the diversity and

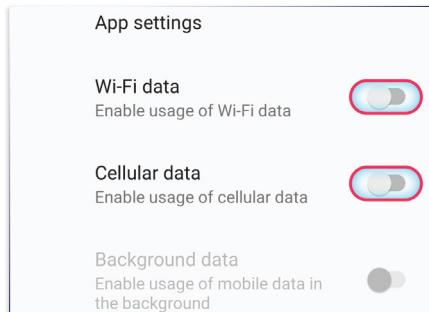
32



33



34



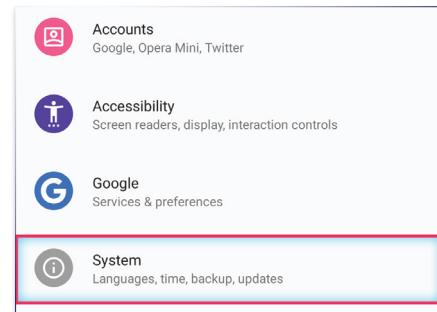
different manufacturers of Android phones and operating systems based on Android, some settings in your phone may differ from those shown in the explanation.

Contact us through technical support accounts to guide you

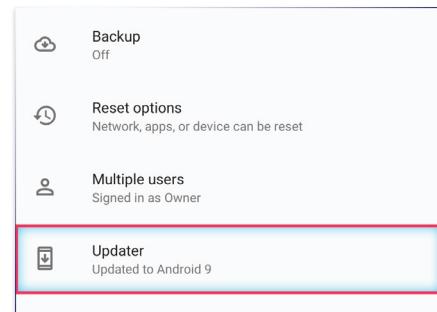
Eighth : Check & Update your phone

Smartphone manufacturers rely on an arbitrary policy to update Android phones, some phones receive monthly security updates and some phones receive every 3 months, so manufacturers do not place user security among their priorities as well as they support Android phones with updates for

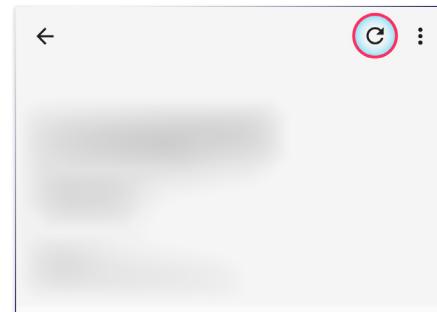
35



36



37



3 years from the date the phone was manufactured - not the date of the phone's purchase - which represents a security problem, as the vulnerabilities are discovered on a daily and permanent basis, and the phone manufacturers make you vulnerable to exploit by hackers and the intelligence agencies

Check your phone for updates regularly, and follow the tech news bulletin issued by Electronic Horizons Foundation to find out the latest vulnerabilities that are being discovered.

36 - Press on " Updater"

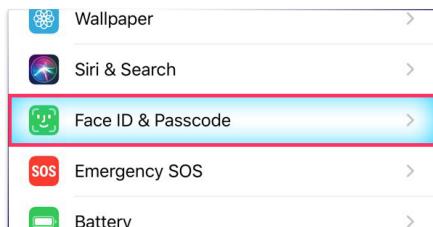
37 - Check for updates



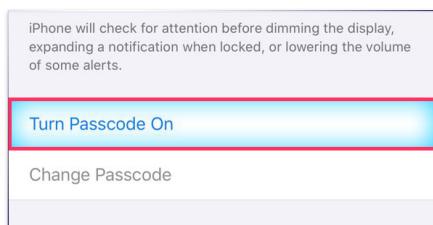
Horizons Designs

Basics of protection in iOS

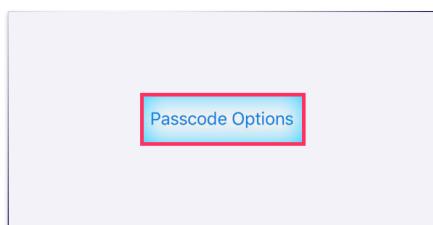
1



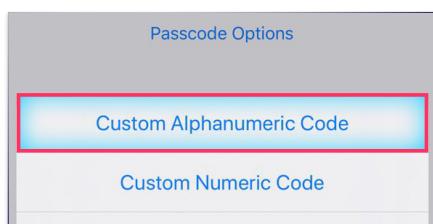
2



3



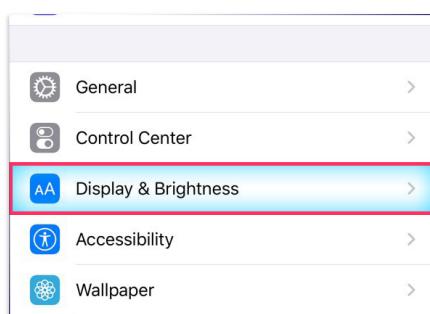
4



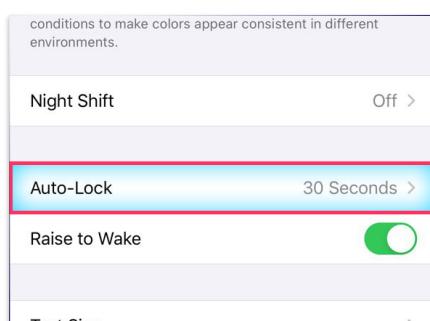
5



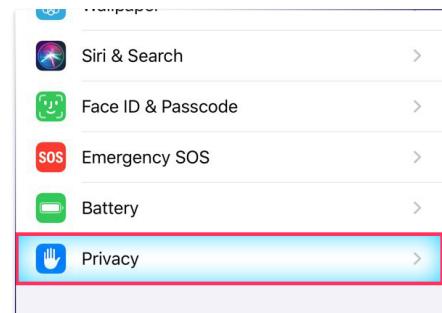
6



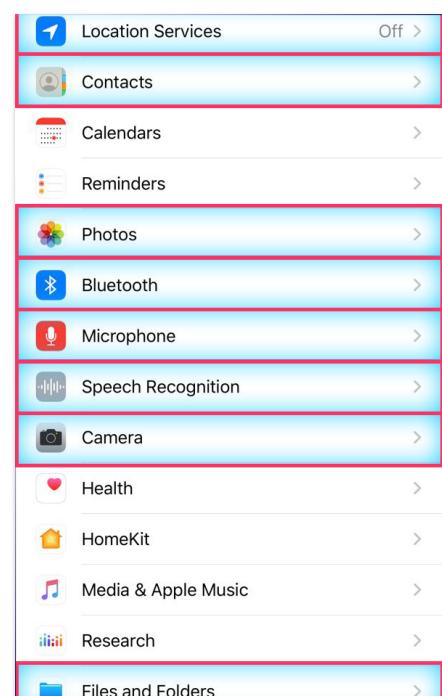
7



8



9



1 | Set a strong passcode

Good iOS security starts with having a really strong passcode. If this is something that's easily guessable then everything else you do is pretty much pointless

- 1- Tap on "Face ID & Passcode"
- 2- Tap on "Turn Passcode On"
- 3- Tap on "Passcode Options"
- 4- Tap on "Custom Alphanumeric Code"

2 | Set brute-force protection

iOS has built-in brute-force

protection to prevent an unauthorized user from trying to guess your passcodes.

5- Go to Settings > Face ID & Passcode ,and scroll down to Erase Data.

3 | Reduce the lock screen timeout

The shorter you set the lock screen timeout setting (there are options ranging from 30 seconds to never), the faster your iPhone or iPad display will require authentication to access it

6- go to "Settings > Display &

Brightness"

7- change the auto-lock time to 30 seconds

4 | Take control over App Permissions

it's possible for any app with access to a device's camera or microphone to spy on you without your knowledge prevent apps from accessing (Camera , GPS , Microphone , Bluetooth , Speech Recognition , Files and Folders , Motion & Fitness , Contacts , Photos)

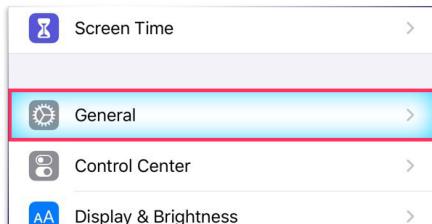
8- go to "Settings > Privacy "

9- change permissions for your apps

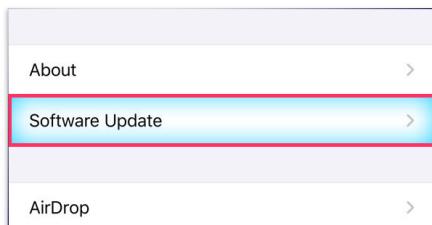
Basics of protection in iOS

iOS

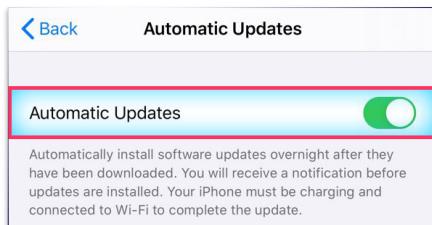
10



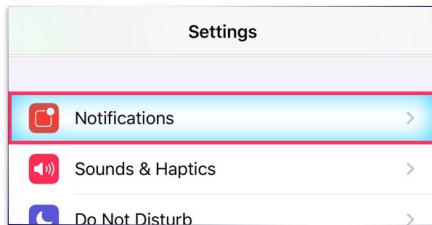
11



12



13



5 | Make sure iOS automatic updates are enabled

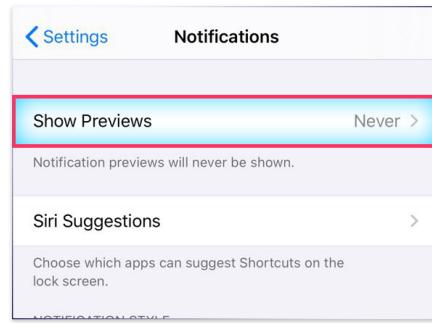
iOS 13 has the ability to keep itself updated automatically, which is a great way to make sure that your iPhone is fully patched

- 10- go to "Settings > General"
- 11- Tap on "Software Update"
- 12- Enable "Automatic Updates"

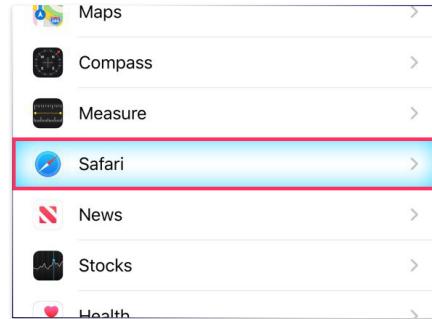
6 | Control notification data leakage

Notifications displayed on the lock screen can leak sensitive

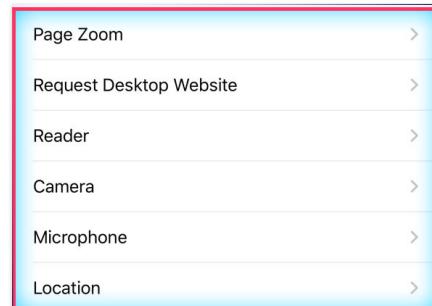
14



15



16



information.

13- go to "Settings > Notifications"

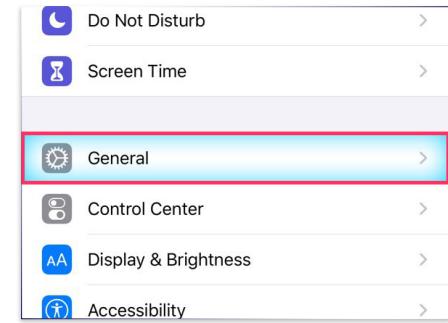
14- Tap on "Show Previews" change the setting to "Never"

7 | Control Websites permissions with Safari

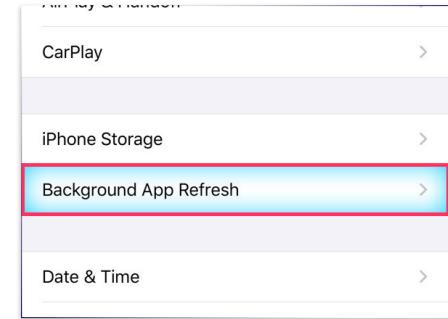
the Safari browser now has the ability to control access to features such as the camera, the microphone, and current location on a per-site basis

- 15- Go to "Settings > Safari"
- 16- Prevent Websites from accessing (Camera , Microphone , Location)

17



18



19



8 | Prevent Background App Refresh

Background refresh is part of what allows any app for iPhone to appear to be multitasking all the time but it could leak your IP address if your VPN Connection dropped So it's recommended to prevent all apps from working in the background and Only allow VPN apps

17- Go to "Settings > General"

18- Tap on "Background App Refresh"

19- Turn off "Background App Refresh"



Wrong security practices

Wrong security practices

Downloading applications from unknown sources exposes your security to the risk of being hacked , where hacked applications are spread on thousands of sites, channels and accounts on social media, the purpose of those applications vary, some of it is developed to target specific people, some just violates your privacy, and sends your data to third parties, and some are developed for random targeting, so you should make sure that the applications and programs that you install and use are downloaded from the official source



Browsing the Internet without using the Tor network or VPN services gives the attacker and the intelligence services the ability to track you and reveal your identity in a few minutes by using the Internet service provider (ISP) in your country, so be sure to use the VPN services as well as the Tor browser to hide your IP



All that an attacker needs to track a person on the Internet is to send a malicious link or website to the target and persuade him to click it so that the attacker can obtain the IP address of your device, which gives him the ability to track you, so make sure to browse any website or link through the Tor browser only



Social networks store every keystroke, every message, and every piece of information on their servers and all the data that you enter, whether you delete them later or not, such as a phone number or email remains stored on the company's servers, and you cannot erase it, so make sure to enter fake Credentials that is not linked to your personal information such as Using virtual number apps to get phone numbers as well as encrypted email services.



Smartphones that do not receive security updates are like a time bomb; attackers can exploit security vulnerabilities in the system to attack you and you cannot patch these vulnerabilities because the manufacturer has stopped supporting your device with security updates. It is recommended to use computers than smart phones and if this is not available, buy a new phone that is supported with Security updates.



Every file, message or image that you sent without encryption can be recovered from your computer or phone if the security agencies got your device, always make sure to encrypt the operating system you are using and the SDcard and USB flash drive before using them



Official social networking applications such as Facebook, Twitter and Instagram contain permissions that violate your privacy and get to know you and your device accurately by accessing your phone's identification data such as (Mac Address - Device ID - IMEI - IMSI) so beware of using social networking applications on your phone and access social media sites through safe browsers.



Using VPN services without activating the permanent connection feature exposes you to the danger of leaking your device's IP address to the applications and browsers that you use or when the system is running which reveals your identity, be sure to activate the permanent connection feature with Always-On services or activate the Kill Switch feature on Windows, Linux and Mac systems



The follower of the weekly technical news bulletin issued by the foundation realizes that the number of discovered vulnerabilities in most programs, applications and operating systems increases every day ignoring security updates exposes you to the risks of being hacked , so be sure to update the applications installed on your phone and the programs installed on your computer and the operating system continuously





Your security
on the internet

We are living in the field of the digital communications revolution. Everything around us is connected to the Internet. The world is changing, and it is moving quickly towards creating a digital infrastructure that depends on collecting information and data about users, and this change and transformation cost you your privacy and security because governments around the world do not care about respecting privacy. We are inside an information war that is open on all fronts, everything is permitted to use with every tool and every means, and you are the only victim of these changes.

China is one of the models that have adopted the creation of digital infrastructure projects in which they rely on the use of modern information-gathering technologies such as “face recognition technology” because it is possible to automatically identify millions of people and store their pictures, data, and movements around the clock, they know where you go and when, and who do you meet.

China was not satisfied with these methods. Rather, it reached more aggressive methods towards the privacy of users, such as banning virtual private network (VPN) services and forcing technical companies to host the content inside servers in China to be able to obtain data for any user inside China, and thus can impose strict censorship. Especially on Muslims inside East Turkestan, they are subject to this type of arbitrary censorship, as well as the Chinese government forces Muslims to install special applications on their phones to monitor conversations and communications on the Internet, but these measures were not implemented by China alone, other governments do the same in other countries, such as «India», which Muslims are subject to a strict censorship to the extent that the establishment of a group on the application of «WhatsApp» requires permission from government agencies!



Some governments in the Middle East countries such as the UAE, Saudi Arabia, and Egypt also use data-processing technologies such as «DPI», which is a type of packet data filter for communications, as governments use it in spying and network surveillance operations such as banning the use of VPN services and redirecting or injecting data packets.

This is an easy glimpse of electronic censorship, whose risks increase day after day, Arab and Western countries are racing to develop tools for collecting information, as this is the information arms race on the Internet.

The intent of information gathering, espionage, and electronic censorship is to stave off any awareness of Muslims within Arab or Western countries. These regimes want you to be just a number that has no power or strength, and compel you to give up your religion and

principles in order to live peacefully under the weight of the feet of the security services!



And that you cannot rise from this profound hibernation without realizing what are you facing. This is an issue that we strive to spread by all means and methods so that Muslims gain sufficient awareness that qualifies them to take correct unobserved steps from the security agencies and achieve the desired destinations - Allah willing

Computer and network security begins with the assumption that there is a field that we can trust, for example if we encrypted data and transmitted over the Internet we generally assume that the device that performs the encryption process is not infiltrated and that the data reaches the required endpoint or destination safely, and until you trust what a particular program does You must trust the underlying operating system running the program. The tasks of the program are limited to what the operating system tells it to do, so you must trust that the operating system prevents leaks of the tasks you are working on for anyone else.

Supporters rely on computers for media work and publishing, starting with design, montage, programming and publishing on social networks, communication, coordination and management of work, and the most popular operating systems that supporters use is Windows developed by Microsoft, which is a security nightmare as it collects all your data, and sends it to Microsoft such as the following:

Sync files are enabled automatically

Sync browsing history and websites

Application and software settings

Wi-Fi network names and passwords



Introduction to computer security

Your device has a unique advertising ID

Microsoft uses the ID to target you with ads through third-party companies and ad networks

Cortana voice assistant can collect any data about you

Voice recordings, search history, and keyboard clicks

Sync the audio files you are listening to

Bank card data synchronization

Sync purchases

Microsoft can collect any data

Sync contacts

Password synchronization

Sync usage data

Sync geolocation data

Sync the content of email messages, programs and audio and video calls

When installing Windows, the user gives Microsoft permission to share any of the above data with third parties without the user's knowledge, and therefore you must use alternative operating systems that maintain your privacy and protect your communications, such as:

-I Qubes OS

An open source security operating system, developed to provide a strong security level for computers, and depends on the principle of isolation into domains that can be controlled through the system. It also supports the operation of various Windows and Linux software

-Γ Tails OS

An improved operating system of the Tor project aims to provide a safe environment for browsing the Internet and bypassing electronic surveillance through the Tor network, and also allows security features including deleting all user data when restarting the device, it is an operating system intended for instant use not for daily use (install Software and data retention) Tails is recommended for sensitive communications and important work coordination.

-¶ Whonix OS

A security operating system that aims to maintain the privacy and security of the user by encrypting data packets through the Tor network and preventing the leakage of an IP address, and can be relied upon in daily use by installing it inside virtualbox on Debian OS

Note: You can use Windows operating system without an Internet connection to use Adobe software in the field of design and montage within the Qubes system or via a virtual system (VM) and use previous systems to communicate, browse and publish.

Install VirtualBox as per the normal mechanism for your .Linux distribution

These instructions are for Debian buster, which is recommended , contact us at technical support accounts to get Debian installation guide

1 | Open terminal and enter this command : sudo apt install wget

```
File Edit View Search Terminal Help
pc@pc:~$ sudo apt install wget
```

2 | Download the Signing Key :

wget https://www.whonix.org/patrick.asc

```
File Edit View Search Terminal Help
pc@pc:~$ wget https://www.whonix.org/patrick.asc
```

3 | Add Whonix's signing key :

sudo apt-key --keyring /etc/apt/trusted.gpg.d/whonix.gpg add ~/patrick.asc

```
File Edit View Search Terminal Help
pc@pc:~$ sudo apt-key --keyring /etc/apt/trusted.gpg.d/whonix.gpg add ~/patrick.asc
```

4 | Add Whonix's APT repository :

echo "deb https://deb.whonix.org buster main contrib non-free" | sudo tee /etc/apt/sources.list.d/whonix.list

```
File Edit View Search Terminal Help
pc@pc:~$ echo "deb https://deb.whonix.org buster main contrib non-free" | sudo tee /etc/apt/sources.list.d/whonix.list
```

5 | Update the package lists : sudo apt-get update

```
File Edit View Search Terminal Help
pc@pc:~$ sudo apt-get update
```

6 | Install VirtualBox and Linux kernel headers :

sudo apt-get install virtualbox linux-headers-\$(dpkg --print-architecture)

```
File Edit View Search Terminal Help
pc@pc:~$ sudo apt-get install virtualbox linux-headers-$(dpkg --print-architecture)
```

7 | Download Whonix from the official website

<https://www.whonix.org/wiki/VirtualBox/Xfce>

then click Download to start

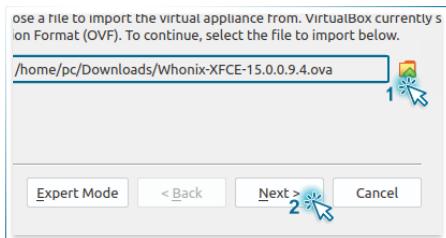
Whonix ™ for VirtualBox with



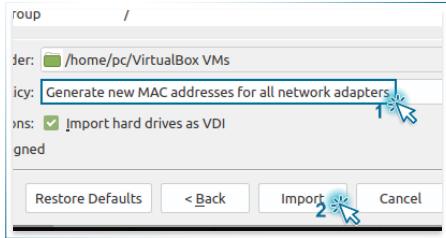
8 | Start VirtualBox from apps menu then press on import



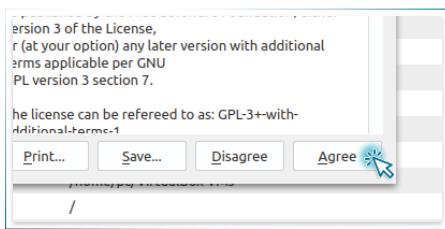
9 | Navigate and select Whonix image and press next



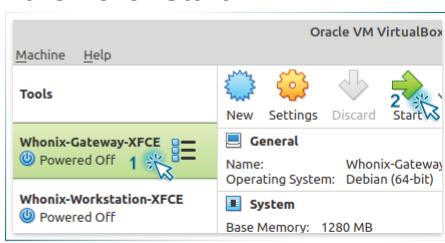
10 | Press on "Mac Address Policy" and select "Generate new MAC addresses for all network adapters" and click on import



11 | Then press "Agree" Wait until Whonix .ova has been imported



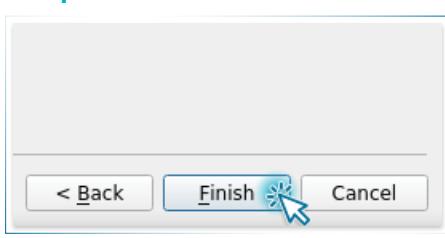
12 | Now start Whonix - Gateway
then click Start



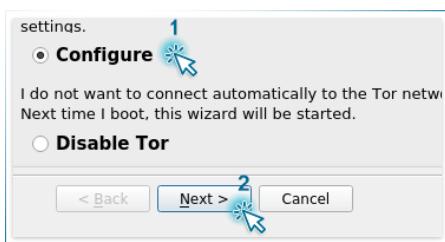
13 | Press on " Understood " then " Next"



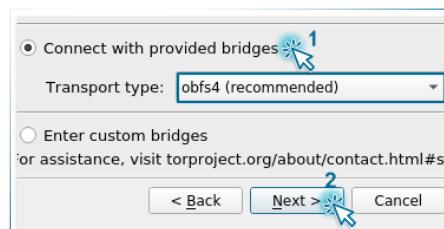
14 | Press on " Finish"



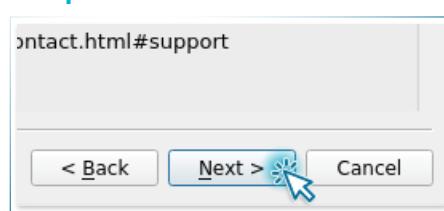
15 | Choose " Configure " to use TOR bridges



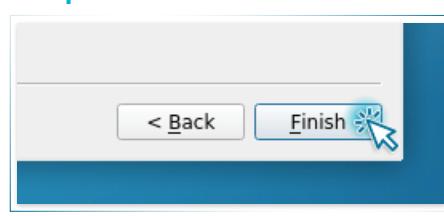
16 | click on " Connect with provided bridges" and choose "obfs4" then press " Next"



17 | Press on " Next"

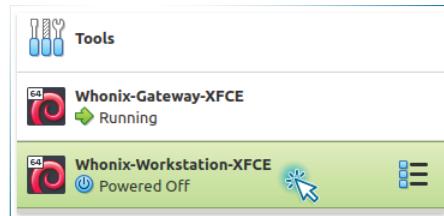


18 | Press on " Finish "

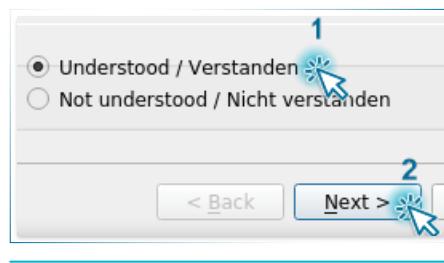


19 | Then start " Whonix - workstation "

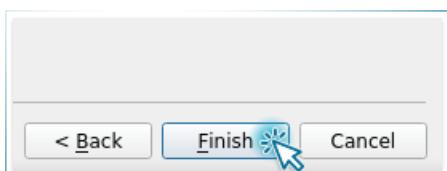
Note : You have to start both Whonix-gateway and Whonix-workstation as whonix gateway anonymize all whonix workstation traffic through TOR network



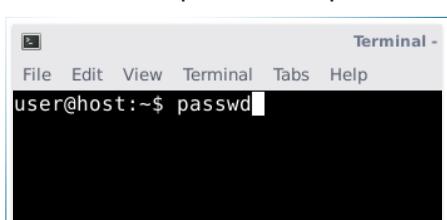
20 | After starting Whonix workstation Press on " Understood " then " Next "



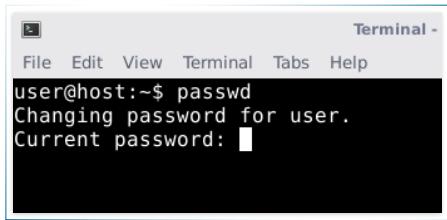
21 | Press on " Finish"



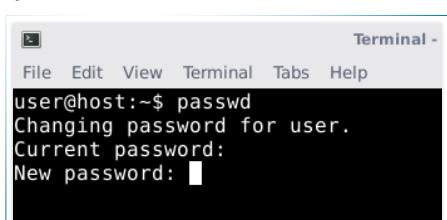
22 | Open Terminal in whonix workstation and enter this command to change the default user password "passwd"



23 | Enter the default password for whonix which is " changeme"



24 | then enter new password for whonix choose a strong password



25 | After you finish setting password enter this command to update whonix

`sudo apt-get-update-plus dist-upgrade`

Note : You should repeat the same steps of changing whonix user password and updating whonix in whonix - gateway

وآخر دعوانا أن الحمد لله
رب العالمين



الحسابات الرسمية لمؤسسة آفاق الإلكترونية

🌐 <https://ehorizons.is>

📠 @ehf:tchnics.de

💬 Horizons@draugr.de

❶ SR444TAW